MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY

P.O. Box 972-60200 – Meru-Kenya.
Tel: +254 (0) 799 529 958, +254 (0) 799 529 959, +254 (0) 712 524 293
Website: www.must.ac.ke Email: info@must.ac.ke

University Examinations 2018/2019

FOURTH YEAR, SPECIAL / SUPPLEMENTARY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE, BACHELOR OF SCIENCE IN COMPUTER TECHNOLOGY AND BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

CCS 3402: COMPUTER SECURITY AND CRYPTOGRAPHY

DATE: SEPTEMBER 2019 **TIME: 2 HOURS**

INSTRUCTIONS: *Answer question **one** and any other **two** questions.*

QUESTION ONE (30 MARKS)

a) Define the following information security terms: (5 Marks)

(i) Exposure
(ii) Attack
(iii) Vulnerability
(iv) Security control
(v) Threats

b) Differentiate between passive and active security attacks. (4 Marks)

c) Explain what a firewall is and briefly explain any two types of firewall. (5 Marks)

d) Explain the following terms as used in ISS. (4 Marks)

(i) Phishing
(ii) Sniffing
(iii) Cryptanalysis
(iv) Cryptography

e) State and briefly explain the two categories of secret key cryptography. (4 Marks)

f) The following cipher text is known to have been encrypted with a Caesar cipher. Determine the key and recover the plaintext.**efgfoeuiffbtuxbmmpguifdbtumf.** (5 Marks)

g) Highlight three ways of dealing with attacks. (3 Marks)

QUESTION TWO (20 MARKS)

a) Explain five firewall design goals. (10 Marks)
b) Differentiate a security plan from a security policy. (5 Marks)
c) State the five services that constitutes to the actual operation of PGP. (5 Marks)
What is the major function of IPsec?

QUESTION THREE (20 MARKS)

a) What is the difference between a block cipher and a stream cipher? (4 Marks)
b) Discuss any two limitations of firewalls. (4 Marks)
c) Discuss how PGP Authentication works. (4 Marks)
d) Explain the following terms as used in ISS.
(i) Phishing
(ii) Sniffing
(iii) Cryptanalysis
(iv) Cryptography (8 Marks)

QUESTION FOUR (20 MARKS)

a) Discuss how the following access control mechanisms work. For each, state any benefits of implementing them. (12 Marks)
(i) Access control lists
(ii) Capability lists
(iii)Role based access control
b) Discuss three goals of a security policy. (6 Marks)
c) What is the difference between an unconditionally secure cipher and a computationally secure cipher? (2 Marks)

QUESTION FIVE (20 MARKS)

a) What are the essential ingredients of a symmetric cipher? (6 Marks)

b) Given Key: 4 3 1 2 5 6 7 using rail fence show how you can encrypt the message “Attack postponed till two AM” (6 Marks)

c) Identify four types of keys used by PGP. (4 Marks)

d) Given ciphertext brute-force cryptanalysis is easily performed on Caesar Cipher. Show how this problem can be solved. (4 Marks)